УДК 004.274:004.056

С.Я. Гільгурт, д.т.н.
Національний авіаційний університет, Київ

ТЕХНІКА ВПОРЯДКУВАННЯ ПАТЕРНІВ ДЛЯ АНАЛІЗУ ТЕХНІЧНИХ ХАРАКТЕРИСТИК РЕКОНФІГУРОВНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У зав'язку зі сталим зростанням мережевого трафіку та кількості кібератак програмна реалізація засобів технічного захисту інформації вже не відповідають вимогам щодо їх швидкодії. Реконфігуровні рішення (на базі ПЛІС) поєднують продуктивність спецпроцесорів і гнучкість програмного забезпечення, тому все частіше використовуються для побудови таких засобів [1].

Схеми апаратного множинного розпізнавання патернів, яке здійснюється в системах технічного захисту інформації на базі сигнатурного (найбільш точного) підходу до розпізнавання, потребують методів кількісної оцінки їх технічних характеристик. Властивості словнику патернів, що входять до складу бази даних сигнатур, мають важливе значення при реалізації таких систем, тому для їх побудови необхідні техніки поводження з патернами.

Подамо множину патернів, що мають розпізнаватися сигнатурною системою захисту інформації, у наступному вигляді:

$$P = \left\{ p_1,\ p_2,\ p_3, \ldots\ p_k, \ldots\ p_\sigma \,\middle|\, \sigma, \Omega, m_{\min}, m_{\max}, \delta, \mu, \mu_z, \nu \right\},$$

де $p_1, p_2, p_3, \ldots p_k, \ldots p_\sigma$, – власне набір патернів, σ – кількість патернів в наборі, Ω – загальна кількість символів в наборі патернів, m_{min} – довжина найкоротшого патерну в наборі, m_{max} – довжина найдовшого патерну в наборі, δ – функція розподілу довжин, μ – перша функція самоподоби, μ_z – перша часткова функція самоподоби, ν – друга функція самоподоби. Патерни p_k є фіксованими послідовностями символів, код кожного з котрих належить до певного алфавіту Σ.

В якості основи подальших розрахунків запропоновано наступну техніку впорядкування патернів у наборі. Відсортуємо всі патерни в множині P за зростанням довжини, як наведено на рис. 1. Складені з квадратів стовпчики зображають рядки символів.

Назвемо *пакетом* сукупність патернів однакової довжини, не звертаючи уваги, як впорядковані патерни всередині сукупності.

Введемо індекс j таким, що співпадає з довжиною патернів в пакеті: $j = m_{min}, m_{min+1}, m_{min+2}, \ldots m_j, \ldots m_{max}$, де m_{min} – довжина найкоротшого патерну, m_{max} – довжина найдовшого патерну, причому кожне наступне значення цього індексу обов'язково на одиницю більше за попереднє, тобто в нумерації немає пропусків.

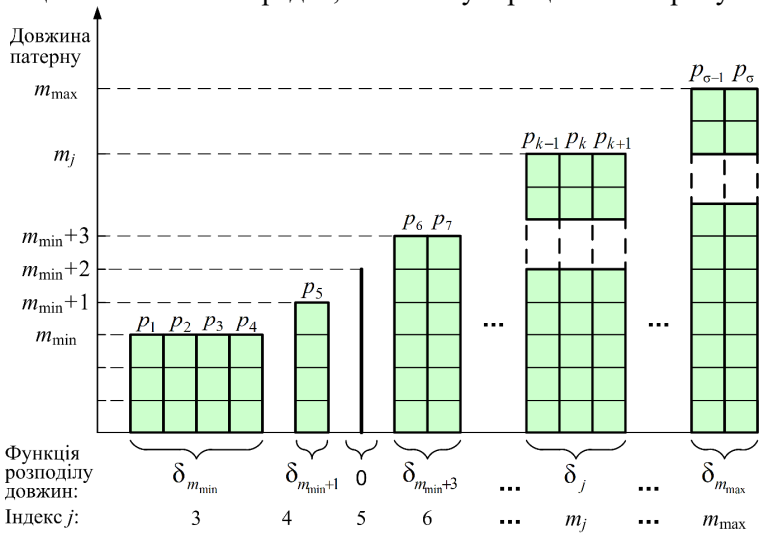

Рис.1. Техніка впорядкування пакетами однакової довжини.

Тоді довжина кожного патерну в наборі співпадатиме з індексом його пакету: $m_j = j$. *Функцію розподілу довжин* δ як залежність від індексу j визначимо рівною кількості патернів у відповідному пакеті: $\delta(j) = \delta_j$. За допомогою цієї функції можна зручно обчислити кількість ненульових пакетів ξ та загальну кількість символів Ω в наборі. Функції самоподоби дозволяють в різний спосіб кількісно оцінювати надмірність словнику патернів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Hilgurt S. A Concise Review of FPGA-Based Hardware Solutions for Network Intrusion Detection. Proceedings of the 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T'2021). – 2021. – Vol. 36. – IEEE, Kharkiv, Ukraine. – P. 164-168.